

# INTRODUCTION

From:

Cathy O'Neil (2017).

*Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.*

New York: Broadway Books.

When I was a little girl, I used to gaze at the traffic out the car window and study the numbers on license plates. I would reduce each one to its basic elements—the prime numbers that made it up.  $45 = 3 \times 3 \times 5$ . That's called factoring, and it was my favorite investigative pastime. As a budding math nerd, I was especially intrigued by the primes.

My love for math eventually became a passion. I went to math camp when I was fourteen and came home clutching a Rubik's Cube to my chest. Math provided a neat refuge from the messiness of the real world. It marched forward, its field of knowledge expanding relentlessly, proof by proof. And I could add to it. I majored in math in college and went on to get my PhD. My thesis was on algebraic number theory, a field with roots in all that

factoring I did as a child. Eventually, I became a tenure-track professor at Barnard, which had a combined math department with Columbia University.

And then I made a big change. I quit my job and went to work as a quant for D. E. Shaw, a leading hedge fund. In leaving academia for finance, I carried mathematics from abstract theory into practice. The operations we performed on numbers translated into trillions of dollars sloshing from one account to another. At first I was excited and amazed by working in this new laboratory, the global economy. But in the autumn of 2008, after I'd been there for a bit more than a year, it came crashing down.

The crash made it all too clear that mathematics, once my refuge, was not only deeply entangled in the world's problems but also fueling many of them. The housing crisis, the collapse of major financial institutions, the rise of unemployment—all had been aided and abetted by mathematicians wielding magic formulas. What's more, thanks to the extraordinary powers that I loved so much, math was able to combine with technology to multiply the chaos and misfortune, adding efficiency and scale to systems that I now recognized as flawed.

If we had been clear-headed, we all would have taken a step back at this point to figure out how math had been misused and how we could prevent a similar catastrophe in the future. But instead, in the wake of the crisis, new mathematical techniques were hotter than ever, and expanding into still more domains. They churned 24/7 through petabytes of information, much of it scraped from social media or e-commerce websites. And increasingly they focused not on the movements of global financial markets but on human beings, on us. Mathematicians and statisticians were studying our desires, movements, and spending power. They were predicting our trustworthiness and calculating our potential as students, workers, lovers, criminals.

This was the Big Data economy, and it promised spectacular gains. A computer program could speed through thousands of résumés or loan applications in a second or two and sort them into neat lists, with the most promising candidates on top. This not only saved time but also was marketed as fair and objective. After all, it didn't involve prejudiced humans digging through reams of paper, just machines processing cold numbers. By 2010 or so, mathematics was asserting itself as never before in human affairs, and the public largely welcomed it.

Yet I saw trouble. The math-powered applications powering the data economy were based on choices made by fallible human beings. Some of these choices were no doubt made with the best intentions. Nevertheless, many of these models encoded human prejudice, misunderstanding, and bias into the software systems that increasingly managed our lives. Like gods, these mathematical models were opaque, their workings invisible to all but the highest priests in their domain: mathematicians and computer scientists. Their verdicts, even when wrong or harmful, were beyond dispute or appeal. And they tended to punish the poor and the oppressed in our society, while making the rich richer.

I came up with a name for these harmful kinds of models: Weapons of Math Destruction, or WMDs for short. I'll walk you through an example, pointing out its destructive characteristics along the way.

As often happens, this case started with a laudable goal. In 2007, Washington, D.C.'s new mayor, Adrian Fenty, was determined to turn around the city's underperforming schools. He had his work cut out for him: at the time, barely one out of every two high school students was surviving to graduation after ninth grade, and only 8 percent of eighth graders were performing at grade level in math. Fenty hired an education reformer named Michelle Rhee to fill a powerful new post, chancellor of Washington's schools.

The going theory was that the students weren't learning enough because their teachers weren't doing a good job. So in 2009, Rhee implemented a plan to weed out the low-performing teachers. This is the trend in troubled school districts around the country, and from a systems engineering perspective the thinking makes perfect sense: Evaluate the teachers. Get rid of the worst ones, and place the best ones where they can do the most good. In the language of data scientists, this "optimizes" the school system, presumably ensuring better results for the kids. Except for "bad" teachers, who could argue with that? Rhee developed a teacher assessment tool called IMPACT, and at the end of the 2009–10 school year the district fired all the teachers whose scores put them in the bottom 2 percent. At the end of the following year, another 5 percent, or 206 teachers, were booted out.

Sarah Wysocki, a fifth-grade teacher, didn't seem to have any reason to worry. She had been at MacFarland Middle School for only two years but was already getting excellent reviews from her principal and her students' parents. One evaluation praised her attentiveness to the children; another called her "one of the best teachers I've ever come into contact with."

Yet at the end of the 2010–11 school year, Wysocki received a miserable score on her IMPACT evaluation. Her problem was a new scoring system known as value-added modeling, which purported to measure her effectiveness in teaching math and language skills. That score, generated by an algorithm, represented half of her overall evaluation, and it outweighed the positive reviews from school administrators and the community. This left the district with no choice but to fire her, along with 205 other teachers who had IMPACT scores below the minimal threshold.

This didn't seem to be a witch hunt or a settling of scores. Indeed, there's a logic to the school district's approach. Admin-

istrators, after all, could be friends with terrible teachers. They could admire their style or their apparent dedication. Bad teachers can *seem* good. So Washington, like many other school systems, would minimize this human bias and pay more attention to scores based on hard results: achievement scores in math and reading. The numbers would speak clearly, district officials promised. They would be more fair.

Wysocki, of course, felt the numbers were horribly unfair, and she wanted to know where they came from. "I don't think anyone understood them," she later told me. How could a good teacher get such dismal scores? What was the value-added model measuring?

Well, she learned, it was complicated. The district had hired a consultancy, Princeton-based Mathematica Policy Research, to come up with the evaluation system. Mathematica's challenge was to measure the educational progress of the students in the district and then to calculate how much of their advance or decline could be attributed to their teachers. This wasn't easy, of course. The researchers knew that many variables, from students' socioeconomic backgrounds to the effects of learning disabilities, could affect student outcomes. The algorithms had to make allowances for such differences, which was one reason they were so complex.

Indeed, attempting to reduce human behavior, performance, and potential to algorithms is no easy job. To understand what Mathematica was up against, picture a ten-year-old girl living in a poor neighborhood in southeastern Washington, D.C. At the end of one school year, she takes her fifth-grade standardized test. Then life goes on. She may have family issues or money problems. Maybe she's moving from one house to another or worried about an older brother who's in trouble with the law. Maybe she's unhappy about her weight or frightened by a bully at school. In

any case, the following year she takes another standardized test, this one designed for sixth graders.

If you compare the results of the tests, the scores should stay stable, or hopefully, jump up. But if her results sink, it's easy to calculate the gap between her performance and that of the successful students.

But how much of that gap is due to her teacher? It's hard to know, and Mathematica's models have only a few numbers to compare. At Big Data companies like Google, by contrast, researchers run constant tests and monitor thousands of variables. They can change the font on a single advertisement from blue to red, serve each version to ten million people, and keep track of which one gets more clicks. They use this feedback to hone their algorithms and fine-tune their operation. While I have plenty of issues with Google, which we'll get to, this type of testing is an effective use of statistics.

Attempting to calculate the impact that one person may have on another over the course of a school year is much more complex. "There are so many factors that go into learning and teaching that it would be very difficult to measure them all," Wysocki says. What's more, attempting to score a teacher's effectiveness by analyzing the test results of only twenty-five or thirty students is statistically unsound, even laughable. The numbers are far too small given all the things that could go wrong. Indeed, if we were to analyze teachers with the statistical rigor of a search engine, we'd have to test them on thousands or even millions of randomly selected students. Statisticians count on large numbers to balance out exceptions and anomalies. (And WMDs, as we'll see, often punish individuals who happen to be the exception.)

Equally important, statistical systems require feedback—something to tell them when they're off track. Statisticians use errors to train their models and make them smarter. If Amazon.com,

through a faulty correlation, started recommending lawn care books to teenage girls, the clicks would plummet, and the algorithm would be tweaked until it got it right. Without feedback, however, a statistical engine can continue spinning out faulty and damaging analysis while never learning from its mistakes.

Many of the WMDs I'll be discussing in this book, including the Washington school district's value-added model, behave like that. They define their own reality and use it to justify their results. This type of model is self-perpetuating, highly destructive—and very common.

When Mathematica's scoring system tags Sarah Wysocki and 205 other teachers as failures, the district fires them. But how does it ever learn if it was right? It doesn't. The system itself has determined that they were failures, and that is how they are viewed. Two hundred and six "bad" teachers are gone. That fact alone appears to demonstrate how effective the value-added model is. It is cleansing the district of underperforming teachers. Instead of searching for the truth, the score comes to embody it.

This is one example of a WMD feedback loop. We'll see many of them throughout this book. Employers, for example, are increasingly using credit scores to evaluate potential hires. Those who pay their bills promptly, the thinking goes, are more likely to show up to work on time and follow the rules. In fact, there are plenty of responsible people and good workers who suffer misfortune and see their credit scores fall. But the belief that bad credit correlates with bad job performance leaves those with low scores less likely to find work. Joblessness pushes them toward poverty, which further worsens their scores, making it even harder for them to land a job. It's a downward spiral. And employers never learn how many good employees they've missed out on by focusing on credit scores. In WMDs, many poisonous assumptions are camouflaged by math and go largely untested and unquestioned.

This underscores another common feature of WMDs. They tend to punish the poor. This is, in part, because they are engineered to evaluate large numbers of people. They specialize in bulk, and they're cheap. That's part of their appeal. The wealthy, by contrast, often benefit from personal input. A white-shoe law firm or an exclusive prep school will lean far more on recommendations and face-to-face interviews than will a fast-food chain or a cash-strapped urban school district. The privileged, we'll see time and again, are processed more by people, the masses by machines.

Wysocki's inability to find someone who could explain her appalling score, too, is telling. Verdicts from WMDs land like dictates from the algorithmic gods. The model itself is a black box, its contents a fiercely guarded corporate secret. This allows consultants like Mathematica to charge more, but it serves another purpose as well: if the people being evaluated are kept in the dark, the thinking goes, they'll be less likely to attempt to game the system. Instead, they'll simply have to work hard, follow the rules, and pray that the model registers and appreciates their efforts. But if the details are hidden, it's also harder to question the score or to protest against it.

For years, Washington teachers complained about the arbitrary scores and clamored for details on what went into them. It's an algorithm, they were told. It's very complex. This discouraged many from pressing further. Many people, unfortunately, are intimidated by math. But a math teacher named Sarah Bax continued to push the district administrator, a former colleague named Jason Kamras, for details. After a back-and-forth that extended for months, Kamras told her to wait for an upcoming technical report. Bax responded: "How do you justify evaluating people by a measure for which you are unable to provide explanation?" But that's the nature of WMDs. The analysis is outsourced to

coders and statisticians. And as a rule, they let the machines do the talking.

Even so, Sarah Wysocki was well aware that her students' standardized test scores counted heavily in the formula. And here she had some suspicions. Before starting what would be her final year at MacFarland Middle School, she had been pleased to see that her incoming fifth graders had scored surprisingly well on their year-end tests. At Barnard Elementary School, where many of Sarah's students came from, 29 percent of the students were ranked at an "advanced reading level." This was five times the average in the school district.

Yet when classes started she saw that many of her students struggled to read even simple sentences. Much later, investigations by the *Washington Post* and *USA Today* revealed a high level of erasures on the standardized tests at forty-one schools in the district, including Barnard. A high rate of corrected answers points to a greater likelihood of cheating. In some of the schools, as many as 70 percent of the classrooms were suspected.

What does this have to do with WMDs? A couple of things. First, teacher evaluation algorithms are a powerful tool for behavioral modification. That's their purpose, and in the Washington schools they featured both a stick and a carrot. Teachers knew that if their students stumbled on the test their own jobs were at risk. This gave teachers a strong motivation to ensure their students passed, especially as the Great Recession battered the labor market. At the same time, if their students outperformed their peers, teachers and administrators could receive bonuses of up to \$8,000. If you add those powerful incentives to the evidence in the case—the high number of erasures and the abnormally high test scores—there were grounds for suspicion that fourth-grade teachers, bowing either to fear or to greed, had corrected their students' exams.

It is conceivable, then, that Sarah Wysocki's fifth-grade students started the school year with artificially inflated scores. If so, their results the following year would make it appear that they'd lost ground in fifth grade—and that their teacher was an underperformer. Wysocki was convinced that this was what had happened to her. That explanation would fit with the observations from parents, colleagues, and her principal that she was indeed a good teacher. It would clear up the confusion. Sarah Wysocki had a strong case to make.

But you cannot appeal to a WMD. That's part of their fearsome power. They do not listen. Nor do they bend. They're deaf not only to charm, threats, and cajoling but also to logic—even when there is good reason to question the data that feeds their conclusions. Yes, if it becomes clear that automated systems are screwing up on an embarrassing and systematic basis, programmers will go back in and tweak the algorithms. But for the most part, the programs deliver unflinching verdicts, and the human beings employing them can only shrug, as if to say, "Hey, what can you do?"

And that is precisely the response Sarah Wysocki finally got from the school district. Jason Kamras later told the *Washington Post* that the erasures were "suggestive" and that the numbers might have been wrong in her fifth-grade class. But the evidence was not conclusive. He said she had been treated fairly.

Do you see the paradox? An algorithm processes a slew of statistics and comes up with a probability that a certain person *might* be a bad hire, a risky borrower, a terrorist, or a miserable teacher. That probability is distilled into a score, which can turn someone's life upside down. And yet when the person fights back, "suggestive" countervailing evidence simply won't cut it. The case must be ironclad. The human victims of WMDs, we'll see time and again, are held to a far higher standard of evidence than the algorithms themselves.

After the shock of her firing, Sarah Wysocki was out of a job for only a few days. She had plenty of people, including her principal, to vouch for her as a teacher, and she promptly landed a position at a school in an affluent district in northern Virginia. So thanks to a highly questionable model, a poor school lost a good teacher, and a rich school, which didn't fire people on the basis of their students' scores, gained one.

...

Following the housing crash, I woke up to the proliferation of WMDs in banking and to the danger they posed to our economy. In early 2011 I quit my job at the hedge fund. Later, after rebranding myself as a data scientist, I joined an e-commerce start-up. From that vantage point, I could see that legions of other WMDs were churning away in every conceivable industry, many of them exacerbating inequality and punishing the poor. They were at the heart of the raging data economy.

To spread the word about WMDs, I launched a blog, Math-Babe. My goal was to mobilize fellow mathematicians against the use of sloppy statistics and biased models that created their own toxic feedback loops. Data specialists, in particular, were drawn to the blog, and they alerted me to the spread of WMDs in new domains. But in mid-2011, when Occupy Wall Street sprang to life in Lower Manhattan, I saw that we had work to do among the broader public. Thousands had gathered to demand economic justice and accountability. And yet when I heard interviews with the Occupiers, they often seemed ignorant of basic issues related to finance. They clearly hadn't been reading my blog. (I should add, though, that you don't need to understand all the details of a system to know that it has failed.)

I could either criticize them or join them, I realized, so I joined them. Soon I was facilitating weekly meetings of the Alternative

Banking Group at Columbia University, where we discussed financial reform. Through this process, I came to see that my two ventures outside academia, one in finance, the other in data science, had provided me with fabulous access to the technology and culture powering WMDs.

Ill-conceived mathematical models now micromanage the economy, from advertising to prisons. These WMDs have many of the same characteristics as the value-added model that derailed Sarah Wysocki's career in Washington's public schools. They're opaque, unquestioned, and unaccountable, and they operate at a scale to sort, target, or "optimize" millions of people. By confusing their findings with on-the-ground reality, most of them create pernicious WMD feedback loops.

But there's one important distinction between a school district's value-added model and, say, a WMD that scouts out prospects for extortionate payday loans. They have different payoffs. For the school district, the payoff is a kind of political currency, a sense that problems are being fixed. But for businesses it's just the standard currency: money. For many of the businesses running these rogue algorithms, the money pouring in seems to prove that their models are working. Look at it through their eyes and it makes sense. When they're building statistical systems to find customers or manipulate desperate borrowers, growing revenue appears to show that they're on the right track. The software is doing its job. The trouble is that profits end up serving as a stand-in, or proxy, for truth. We'll see this dangerous confusion crop up again and again.

This happens because data scientists all too often lose sight of the folks on the receiving end of the transaction. They certainly understand that a data-crunching program is bound to misinterpret people a certain percentage of the time, putting them in the wrong groups and denying them a job or a chance at their dream

house. But as a rule, the people running the WMDs don't dwell on those errors. Their feedback is money, which is also their incentive. Their systems are engineered to gobble up more data and fine-tune their analytics so that more money will pour in. Investors, of course, feast on these returns and shower WMD companies with more money.

And the victims? Well, an internal data scientist might say, no statistical system can be *perfect*. Those folks are collateral damage. And often, like Sarah Wysocki, they are deemed unworthy and expendable. Forget about them for a minute, they might say, and focus on all the people who get helpful suggestions from recommendation engines or who find music they love on Pandora, the ideal job on LinkedIn, or perhaps the love of their life on Match.com. Think of the astounding scale, and ignore the imperfections.

Big Data has plenty of evangelists, but I'm not one of them. This book will focus sharply in the other direction, on the damage inflicted by WMDs and the injustice they perpetuate. We will explore harmful examples that affect people at critical life moments: going to college, borrowing money, getting sentenced to prison, or finding and holding a job. All of these life domains are increasingly controlled by secret models wielding arbitrary punishments.

Welcome to the dark side of Big Data.

1



## BOMB PARTS

### What Is a Model?

It was a hot August afternoon in 1946. Lou Boudreau, the player-manager of the Cleveland Indians, was having a miserable day. In the first game of a doubleheader, Ted Williams had almost single-handedly annihilated his team. Williams, perhaps the game's greatest hitter at the time, had smashed three home runs and driven home eight. The Indians ended up losing 11 to 10.

Boudreau had to take action. So when Williams came up for the first time in the second game, players on the Indians' side started moving around. Boudreau, the shortstop, jogged over to where the second baseman would usually stand, and the second baseman backed into short right field. The third baseman moved

to his left, into the shortstop's hole. It was clear that Boudreau, perhaps out of desperation, was shifting the entire orientation of his defense in an attempt to turn Ted Williams's hits into outs.

In other words, he was thinking like a data scientist. He had analyzed crude data, most of it observational: Ted Williams *usually* hit the ball to right field. Then he adjusted. And it worked. Fielders caught more of Williams's blistering line drives than before (though they could do nothing about the home runs sailing over their heads).

If you go to a major league baseball game today, you'll see that defenses now treat nearly every player like Ted Williams. While Boudreau merely observed where Williams usually hit the ball, managers now know precisely where every player has hit every ball over the last week, over the last month, throughout his career, against left-handers, when he has two strikes, and so on. Using this historical data, they analyze their current situation and calculate the positioning that is associated with the highest probability of success. And that sometimes involves moving players far across the field.

Shifting defenses is only one piece of a much larger question: What steps can baseball teams take to maximize the probability that they'll win? In their hunt for answers, baseball statisticians have scrutinized every variable they can quantify and attached it to a value. How much more is a double worth than a single? When, if ever, is it worth it to bunt a runner from first to second base?

The answers to all of these questions are blended and combined into mathematical models of their sport. These are parallel universes of the baseball world, each a complex tapestry of probabilities. They include every measurable relationship among every one of the sport's components, from walks to home runs to the players themselves. The purpose of the model is to run different

scenarios at every juncture, looking for the optimal combinations. If the Yankees bring in a right-handed pitcher to face Angels slugger Mike Trout, as compared to leaving in the current pitcher, how much more likely are they to get him out? And how will that affect their overall odds of winning?

Baseball is an ideal home for predictive mathematical modeling. As Michael Lewis wrote in his 2003 bestseller, *Moneyball*, the sport has attracted data nerds throughout its history. In decades past, fans would pore over the stats on the back of baseball cards, analyzing Carl Yastrzemski's home run patterns or comparing Roger Clemens's and Dwight Gooden's strikeout totals. But starting in the 1980s, serious statisticians started to investigate what these figures, along with an avalanche of new ones, really meant: how they translated into wins, and how executives could maximize success with a minimum of dollars.

"Moneyball" is now shorthand for any statistical approach in domains long ruled by the gut. But baseball represents a healthy case study—and it serves as a useful contrast to the toxic models, or WMDs, that are popping up in so many areas of our lives. Baseball models are fair, in part, because they're transparent. Everyone has access to the stats and can understand more or less how they're interpreted. Yes, one team's model might give more value to home run hitters, while another might discount them a bit, because sluggers tend to strike out a lot. But in either case, the numbers of home runs and strikeouts are there for everyone to see.

Baseball also has statistical rigor. Its gurus have an immense data set at hand, almost all of it directly related to the performance of players in the game. Moreover, their data is highly relevant to the outcomes they are trying to predict. This may sound obvious, but as we'll see throughout this book, the folks building WMDs routinely lack data for the behaviors they're most interested in. So they substitute stand-in data, or proxies. They draw statistical

correlations between a person's zip code or language patterns and her potential to pay back a loan or handle a job. These correlations are discriminatory, and some of them are illegal. Baseball models, for the most part, don't use proxies because they use pertinent inputs like balls, strikes, and hits.

Most crucially, that data is constantly pouring in, with new statistics from an average of twelve or thirteen games arriving daily from April to October. Statisticians can compare the results of these games to the predictions of their models, and they can see where they were wrong. Maybe they predicted that a left-handed reliever would give up lots of hits to right-handed batters—and yet he mowed them down. If so, the stats team has to tweak their model and also carry out research on why they got it wrong. Did the pitcher's new screwball affect his statistics? Does he pitch better at night? Whatever they learn, they can feed back into the model, refining it. That's how trustworthy models operate: They maintain a constant back-and-forth with whatever in the world they're trying to understand or predict. Conditions change, and so must the model.

Now, you may look at the baseball model, with its thousands of changing variables, and wonder how we could even be comparing it to the model used to evaluate teachers in Washington, D.C., schools. In one of them, an entire sport is modeled in fastidious detail and updated continuously. The other, while cloaked in mystery, appears to lean heavily on a handful of test results from one year to the next. Is that really a model?

The answer is yes. A model, after all, is nothing more than an abstract representation of some process, be it a baseball game, an oil company's supply chain, a foreign government's actions, or a movie theater's attendance. Whether it's running in a computer program or in our head, the model takes what we know and uses it to predict responses in various situations. All of us carry thousands

of models in our heads. They tell us what to expect, and they guide our decisions.

Here's an informal model I use every day. As a mother of three, I cook the meals at home—my husband, bless his heart, cannot remember to put salt in pasta water. Each night when I begin to cook a family meal, I internally and intuitively model everyone's appetite. I know that one of my sons loves chicken (but hates hamburgers), while another will eat only the pasta (with extra grated parmesan cheese). But I also have to take into account that people's appetites vary from day to day, so a change can catch my model by surprise. There's some unavoidable uncertainty involved.

The input to my internal cooking model is the information I have about my family, the ingredients I have on hand or I know are available, and my own energy, time, and ambition. The output is how and what I decide to cook. I evaluate the success of a meal by how satisfied my family seems at the end of it, how much they've eaten, and how healthy the food was. Seeing how well it is received and how much of it is enjoyed allows me to update my model for the next time I cook. The updates and adjustments make it what statisticians call a "dynamic model."

Over the years I've gotten pretty good at making meals for my family, I'm proud to say. But what if my husband and I go away for a week, and I want to explain my system to my mom so she can fill in for me? Or what if my friend who has kids wants to know my methods? That's when I'd start to formalize my model, making it much more systematic and, in some sense, mathematical. And if I were feeling ambitious, I might put it into a computer program.

Ideally, the program would include all of the available food options, their nutritional value and cost, and a complete database of my family's tastes: each individual's preferences and aversions. It would be hard, though, to sit down and summon all that

information off the top of my head. I've got loads of memories of people grabbing seconds of asparagus or avoiding the string beans. But they're all mixed up and hard to formalize in a comprehensive list.

The better solution would be to train the model over time, entering data every day on what I'd bought and cooked and noting the responses of each family member. I would also include parameters, or constraints. I might limit the fruits and vegetables to what's in season and dole out a certain amount of Pop-Tarts, but only enough to forestall an open rebellion. I also would add a number of rules. This one likes meat, this one likes bread and pasta, this one drinks lots of milk and insists on spreading Nutella on everything in sight.

If I made this work a major priority, over many months I might come up with a very good model. I would have turned the food management I keep in my head, my informal internal model, into a formal external one. In creating my model, I'd be extending my power and influence in the world. I'd be building an automated me that others can implement, even when I'm not around.

There would always be mistakes, however, because models are, by their very nature, simplifications. No model can include all of the real world's complexity or the nuance of human communication. Inevitably, some important information gets left out. I might have neglected to inform my model that junk-food rules are relaxed on birthdays, or that raw carrots are more popular than the cooked variety.

To create a model, then, we make choices about what's important enough to include, simplifying the world into a toy version that can be easily understood and from which we can infer important facts and actions. We expect it to handle only one job and accept that it will occasionally act like a clueless machine, one with enormous blind spots.

Sometimes these blind spots don't matter. When we ask Google Maps for directions, it models the world as a series of roads, tunnels, and bridges. It ignores the buildings, because they aren't relevant to the task. When avionics software guides an airplane, it models the wind, the speed of the plane, and the landing strip below, but not the streets, tunnels, buildings, and people.

A model's blind spots reflect the judgments and priorities of its creators. While the choices in Google Maps and avionics software appear cut and dried, others are far more problematic. The value-added model in Washington, D.C., schools, to return to that example, evaluates teachers largely on the basis of students' test scores, while ignoring how much the teachers engage the students, work on specific skills, deal with classroom management, or help students with personal and family problems. It's overly simple, sacrificing accuracy and insight for efficiency. Yet from the administrators' perspective it provides an effective tool to ferret out hundreds of apparently underperforming teachers, even at the risk of misreading some of them.

Here we see that models, despite their reputation for impartiality, reflect goals and ideology. When I removed the possibility of eating Pop-Tarts at every meal, I was imposing my ideology on the meals model. It's something we do without a second thought. Our own values and desires influence our choices, from the data we choose to collect to the questions we ask. Models are opinions embedded in mathematics.

Whether or not a model works is also a matter of opinion. After all, a key component of every model, whether formal or informal, is its definition of success. This is an important point that we'll return to as we explore the dark world of WMDs. In each case, we must ask not only who designed the model but also what that person or company is trying to accomplish. If the North Korean government built a model for my family's meals, for example, it

might be optimized to keep us above the threshold of starvation at the lowest cost, based on the food stock available. Preferences would count for little or nothing. By contrast, if my kids were creating the model, success might feature ice cream at every meal. My own model attempts to blend a bit of the North Koreans' resource management with the happiness of my kids, along with my own priorities of health, convenience, diversity of experience, and sustainability. As a result, it's much more complex. But it still reflects my own personal reality. And a model built for today will work a bit worse tomorrow. It will grow stale if it's not constantly updated. Prices change, as do people's preferences. A model built for a six-year-old won't work for a teenager.

This is true of internal models as well. You can often see troubles when grandparents visit a grandchild they haven't seen for a while. On their previous visit, they gathered data on what the child knows, what makes her laugh, and what TV show she likes and (unconsciously) created a model for relating to this particular four-year-old. Upon meeting her a year later, they can suffer a few awkward hours because their models are out of date. Thomas the Tank Engine, it turns out, is no longer cool. It takes some time to gather new data about the child and adjust their models.

This is not to say that good models cannot be primitive. Some very effective ones hinge on a single variable. The most common model for detecting fires in a home or office weighs only one strongly correlated variable, the presence of smoke. That's usually enough. But modelers run into problems—or subject us to problems—when they focus models as simple as a smoke alarm on their fellow humans.

Racism, at the individual level, can be seen as a predictive model whirring away in billions of human minds around the world. It is built from faulty, incomplete, or generalized data. Whether it comes from experience or hearsay, the data indicates

that certain types of people have behaved badly. That generates a binary prediction that all people of that race will behave that same way.

Needless to say, racists don't spend a lot of time hunting down reliable data to train their twisted models. And once their model morphs into a belief, it becomes hardwired. It generates poisonous assumptions, yet rarely tests them, settling instead for data that seems to confirm and fortify them. Consequently, racism is the most slovenly of predictive models. It is powered by haphazard data gathering and spurious correlations, reinforced by institutional inequities, and polluted by confirmation bias. In this way, oddly enough, racism operates like many of the WMDs I'll be describing in this book.

• • •

In 1997, a convicted murderer, an African American man named Duane Buck, stood before a jury in Harris County, Texas. Buck had killed two people, and the jury had to decide whether he would be sentenced to death or to life in prison with the chance of parole. The prosecutor pushed for the death penalty, arguing that if Buck were let free he might kill again.

Buck's defense attorney brought forth an expert witness, a psychologist named Walter Quijano, who didn't help his client's case one bit. Quijano, who had studied recidivism rates in the Texas prison system, made a reference to Buck's race, and during cross-examination the prosecutor jumped on it.

"You have determined that the . . . the race factor, black, increases the future dangerousness for various complicated reasons. Is that correct?" the prosecutor asked.

"Yes," Quijano answered. The prosecutor stressed that testimony in her summation, and the jury sentenced Buck to death.

Three years later, Texas attorney general John Cornyn found

that the psychologist had given similar race-based testimony in six other capital cases, most of them while he worked for the prosecution. Cornyn, who would be elected in 2002 to the US Senate, ordered new race-blind hearings for the seven inmates. In a press release, he declared: “It is inappropriate to allow race to be considered as a factor in our criminal justice system. . . . The people of Texas want and deserve a system that affords the same fairness to everyone.”

Six of the prisoners got new hearings but were again sentenced to death. Quijano’s prejudicial testimony, the court ruled, had not been decisive. Buck never got a new hearing, perhaps because it was his own witness who had brought up race. He is still on death row.

Regardless of whether the issue of race comes up explicitly at trial, it has long been a major factor in sentencing. A University of Maryland study showed that in Harris County, which includes Houston, prosecutors were three times more likely to seek the death penalty for African Americans, and four times more likely for Hispanics, than for whites convicted of the same charges. That pattern isn’t unique to Texas. According to the American Civil Liberties Union, sentences imposed on black men in the federal system are nearly 20 percent longer than those for whites convicted of similar crimes. And though they make up only 13 percent of the population, blacks fill up 40 percent of America’s prison cells.

So you might think that computerized risk models fed by data would reduce the role of prejudice in sentencing and contribute to more even-handed treatment. With that hope, courts in twenty-four states have turned to so-called recidivism models. These help judges assess the danger posed by each convict. And by many measures they’re an improvement. They keep sentences more consistent and less likely to be swayed by the moods and bi-

ases of judges. They also save money by nudging down the length of the average sentence. (It costs an average of \$31,000 a year to house an inmate, and double that in expensive states like Connecticut and New York.)

The question, however, is whether we’ve eliminated human bias or simply camouflaged it with technology. The new recidivism models are complicated and mathematical. But embedded within these models are a host of assumptions, some of them prejudicial. And while Walter Quijano’s words were transcribed for the record, which could later be read and challenged in court, the workings of a recidivism model are tucked away in algorithms, intelligible only to a tiny elite.

One of the more popular models, known as LSI-R, or Level of Service Inventory-Revised, includes a lengthy questionnaire for the prisoner to fill out. One of the questions—“How many prior convictions have you had?”—is highly relevant to the risk of recidivism. Others are also clearly related: “What part did others play in the offense? What part did drugs and alcohol play?”

But as the questions continue, delving deeper into the person’s life, it’s easy to imagine how inmates from a privileged background would answer one way and those from tough inner-city streets another. Ask a criminal who grew up in comfortable suburbs about “the first time you were ever involved with the police,” and he might not have a single incident to report other than the one that brought him to prison. Young black males, by contrast, are likely to have been stopped by police dozens of times, even when they’ve done nothing wrong. A 2013 study by the New York Civil Liberties Union found that while black and Latino males between the ages of fourteen and twenty-four made up only 4.7 percent of the city’s population, they accounted for 40.6 percent of the stop-and-frisk checks by police. More than 90 percent of those stopped were innocent. Some of the others might have been drinking underage

or carrying a joint. And unlike most rich kids, they got in trouble for it. So if early “involvement” with the police signals recidivism, poor people and racial minorities look far riskier.

The questions hardly stop there. Prisoners are also asked about whether their friends and relatives have criminal records. Again, ask that question to a convicted criminal raised in a middle-class neighborhood, and the chances are much greater that the answer will be no. The questionnaire does avoid asking about race, which is illegal. But with the wealth of detail each prisoner provides, that single illegal question is almost superfluous.

The LSI-R questionnaire has been given to thousands of inmates since its invention in 1995. Statisticians have used those results to devise a system in which answers highly correlated to recidivism weigh more heavily and count for more points. After answering the questionnaire, convicts are categorized as high, medium, and low risk on the basis of the number of points they accumulate. In some states, such as Rhode Island, these tests are used only to target those with high-risk scores for antirecidivism programs while incarcerated. But in others, including Idaho and Colorado, judges use the scores to guide their sentencing.

This is unjust. The questionnaire includes circumstances of a criminal’s birth and upbringing, including his or her family, neighborhood, and friends. These details should not be relevant to a criminal case or to the sentencing. Indeed, if a prosecutor attempted to tar a defendant by mentioning his brother’s criminal record or the high crime rate in his neighborhood, a decent defense attorney would roar, “Objection, Your Honor!” And a serious judge would sustain it. This is the basis of our legal system. We are judged by what we do, not by who we are. And although we don’t know the exact weights that are attached to these parts of the test, any weight above zero is unreasonable.

Many would point out that statistical systems like the LSI-R

are effective in gauging recidivism risk—or at least more accurate than a judge’s random guess. But even if we put aside, ever so briefly, the crucial issue of fairness, we find ourselves descending into a pernicious WMD feedback loop. A person who scores as “high risk” is likely to be unemployed and to come from a neighborhood where many of his friends and family have had run-ins with the law. Thanks in part to the resulting high score on the evaluation, he gets a longer sentence, locking him away for more years in a prison where he’s surrounded by fellow criminals—which raises the likelihood that he’ll return to prison. He is finally released into the same poor neighborhood, this time with a criminal record, which makes it that much harder to find a job. If he commits another crime, the recidivism model can claim another success. But in fact the model itself contributes to a toxic cycle and helps to sustain it. That’s a signature quality of a WMD.

...

In this chapter, we’ve looked at three kinds of models. The baseball models, for the most part, are healthy. They are transparent and continuously updated, with both the assumptions and the conclusions clear for all to see. The models feed on statistics from the game in question, not from proxies. And the people being modeled understand the process and share the model’s objective: winning the World Series. (Which isn’t to say that many players, come contract time, won’t quibble with a model’s valuations: “Sure I struck out two hundred times, but look at my *home runs* . . .”)

From my vantage point, there’s certainly nothing wrong with the second model we discussed, the hypothetical family meal model. If my kids were to question the assumptions that underlie it, whether economic or dietary, I’d be all too happy to provide them. And even though they sometimes grouse when facing

something green, they'd likely admit, if pressed, that they share the goals of convenience, economy, health, and good taste—though they might give them different weights in their own models. (And they'll be free to create them when they start buying their own food.)

I should add that my model is highly unlikely to scale. I don't see Walmart or the US Agriculture Department or any other titan embracing my app and imposing it on hundreds of millions of people, like some of the WMDs we'll be discussing. No, my model is benign, especially since it's unlikely ever to leave my head and be formalized into code.

The recidivism example at the end of the chapter, however, is a different story entirely. It gives off a familiar and noxious odor. So let's do a quick exercise in WMD taxonomy and see where it fits.

The first question: Even if the participant is aware of being modeled, or what the model is used for, is the model opaque, or even invisible? Well, most of the prisoners filling out mandatory questionnaires aren't stupid. They at least have reason to suspect that information they provide will be used against them to control them while in prison and perhaps lock them up for longer. They know the game. But prison officials know it, too. And they keep quiet about the purpose of the LSI-R questionnaire. Otherwise, they know, many prisoners will attempt to game it, providing answers to make them look like model citizens the day they leave the joint. So the prisoners are kept in the dark as much as possible and do not learn their risk scores.

In this, they're hardly alone. Opaque and invisible models are the rule, and clear ones very much the exception. We're modeled as shoppers and couch potatoes, as patients and loan applicants, and very little of this do we see—even in applications we happily sign up for. Even when such models behave themselves, opacity can lead to a feeling of unfairness. If you were told by an usher,

upon entering an open-air concert, that you couldn't sit in the first ten rows of seats, you might find it unreasonable. But if it were explained to you that the first ten rows were being reserved for people in wheelchairs, then it might well make a difference. Transparency matters.

And yet many companies go out of their way to hide the results of their models or even their existence. One common justification is that the algorithm constitutes a "secret sauce" crucial to their business. It's *intellectual property*, and it must be defended, if need be, with legions of lawyers and lobbyists. In the case of web giants like Google, Amazon, and Facebook, these precisely tailored algorithms alone are worth hundreds of billions of dollars. WMDs are, by design, inscrutable black boxes. That makes it extra hard to definitively answer the second question: Does the model work against the subject's interest? In short, is it unfair? Does it damage or destroy lives?

Here, the LSI-R again easily qualifies as a WMD. The people putting it together in the 1990s no doubt saw it as a tool to bring evenhandedness and efficiency to the criminal justice system. It could also help nonthreatening criminals land lighter sentences. This would translate into more years of freedom for them and enormous savings for American taxpayers, who are footing a \$70 billion annual prison bill. However, because the questionnaire judges the prisoner by details that would not be admissible in court, it is unfair. While many may benefit from it, it leads to suffering for others.

A key component of this suffering is the pernicious feedback loop. As we've seen, sentencing models that profile a person by his or her circumstances help to create the environment that justifies their assumptions. This destructive loop goes round and round, and in the process the model becomes more and more unfair.

The third question is whether a model has the capacity to grow

exponentially. As a statistician would put it, can it scale? This might sound like the nerdy quibble of a mathematician. But scale is what turns WMDs from local nuisances into tsunami forces, ones that define and delimit our lives. As we'll see, the developing WMDs in human resources, health, and banking, just to name a few, are quickly establishing broad norms that exert upon us something very close to the power of law. If a bank's model of a high-risk borrower, for example, is applied to you, the world will treat you as just that, a deadbeat—even if you're horribly misunderstood. And when that model scales, as the credit model has, it affects your whole life—whether you can get an apartment or a job or a car to get from one to the other.

When it comes to scaling, the potential for recidivism modeling continues to grow. It's already used in the majority of states, and the LSI-R is the most common tool, used in at least twenty-one of them. Beyond LSI-R, prisons host a lively and crowded market for data scientists. The penal system is teeming with data, especially since convicts enjoy even fewer privacy rights than the rest of us. What's more, the system is so miserable, overcrowded, inefficient, expensive, and inhumane that it's crying out for improvements. Who wouldn't want a cheap solution like this?

Penal reform is a rarity in today's polarized political world, an issue on which liberals and conservatives are finding common ground. In early 2015, the conservative Koch brothers, Charles and David, teamed up with a liberal think tank, the Center for American Progress, to push for prison reform and drive down the incarcerated population. But my suspicion is this: their bipartisan effort to reform prisons, along with legions of others, is almost certain to lead to the efficiency and perceived fairness of a data-fed solution. That's the age we live in. Even if other tools supplant LSI-R as its leading WMD, the prison system is likely to be a powerful incubator for WMDs on a grand scale.

So to sum up, these are the three elements of a WMD: Opacity, Scale, and Damage. All of them will be present, to one degree or another, in the examples we'll be covering. Yes, there will be room for quibbles. You could argue, for example, that the recidivism scores are not totally opaque, since they spit out scores that prisoners, in some cases, can see. Yet they're brimming with mystery, since the prisoners cannot see how their answers produce their score. The scoring algorithm is hidden. A couple of the other WMDs might not seem to satisfy the prerequisite for scale. They're not huge, at least not yet. But they represent dangerous species that are primed to grow, perhaps exponentially. So I count them. And finally, you might note that not all of these WMDs are universally damaging. After all, they send some people to Harvard, line others up for cheap loans or good jobs, and reduce jail sentences for certain lucky felons. But the point is not whether some people benefit. It's that so many suffer. These models, powered by algorithms, slam doors in the face of millions of people, often for the flimsiest of reasons, and offer no appeal. They're unfair.

And here's one more thing about algorithms: they can leap from one field to the next, and they often do. Research in epidemiology can hold insights for box office predictions; spam filters are being retooled to identify the AIDS virus. This is true of WMDs as well. So if mathematical models in prisons appear to succeed at their job—which really boils down to efficient management of people—they could spread into the rest of the economy along with the other WMDs, leaving us as collateral damage.

That's my point. This menace is rising. And the world of finance provides a cautionary tale.

# CONCLUSION

In this march through a virtual lifetime, we've visited school and college, the courts and the workplace, even the voting booth. Along the way, we've witnessed the destruction caused by WMDs. Promising efficiency and fairness, they distort higher education, drive up debt, spur mass incarceration, pummel the poor at nearly every juncture, and undermine democracy. It might seem like the logical response is to disarm these weapons, one by one.

The problem is that they're feeding on each other. Poor people are more likely to have bad credit and live in high-crime neighborhoods, surrounded by other poor people. Once the dark universe of WMDs digests that data, it showers them with predatory ads for subprime loans or for-profit schools. It sends more police to arrest them, and when they're convicted it sentences them to longer

terms. This data feeds into other WMDs, which score the same people as high risks or easy targets and proceed to block them from jobs, while jacking up their rates for mortgages, car loans, and every kind of insurance imaginable. This drives their credit rating down further, creating nothing less than a death spiral of modeling. Being poor in a world of WMDs is getting more and more dangerous and expensive.

The same WMDs that abuse the poor also place the comfortable classes of society in their own marketing silos. They jet them off to vacations in Aruba and wait-list them at Wharton. For many of them, it can feel as though the world is getting smarter and easier. Models highlight bargains on prosciutto and chianti, recommend a great movie on Amazon Prime, or lead them, turn by turn, to a café in what used to be a “sketchy” neighborhood. The quiet and personal nature of this targeting keeps society’s winners from seeing how the very same models are destroying lives, sometimes just a few blocks away.

Our national motto, *E Pluribus Unum*, means “Out of Many, One.” But WMDs reverse the equation. Working in darkness, they carve one into many, while hiding us from the harms they inflict upon our neighbors near and far. And those harms are legion. They unfold when a single mother can’t arrange child care fast enough to adapt to her work schedule, or when a struggling young person is red-lighted for an hourly job by a workplace personality test. We see them when a poor minority teenager gets stopped, roughed up, and put on warning by the local police, or when a gas station attendant who lives in a poor zip code gets hit with a higher insurance bill. It’s a silent war that hits the poor hardest but also hammers the middle class. Its victims, for the most part, lack economic power, access to lawyers, or well-funded political organizations to fight their battles. The result is widespread damage that all too often passes for inevitability.

We cannot count on the free market itself to right these wrongs. To understand why, let’s compare WMDs to another scourge our society has been grappling with, homophobia.

In September of 1996, two months before his reelection, President Bill Clinton signed the Defense of Marriage Act. This law, defining marriage as between one man and one woman, promised to firm up support for the president in conservative patches of battleground states, including Ohio and Florida.

Only a week later, the tech giant IBM announced that it would provide medical benefits to the same-sex partners of its employees. You might wonder why Big Blue, a pillar of the corporate establishment, would open this door and invite controversy when a putatively progressive American president was moving in the opposite direction.

The answer has to do with the bottom line. In 1996, the Internet gold rush was just taking off, and IBM was battling for brainpower with Oracle, Microsoft, Hewlett-Packard, and a host of start-ups, including Amazon and Yahoo. Most of those other companies were already providing benefits to same-sex partners and attracting gay and lesbian talent. IBM could not afford to miss out. “In terms of business competitiveness, it made sense for us,” an IBM spokesperson told *BusinessWeek* at the time.

If we think about human resources policies at IBM and other companies as algorithms, they codified discrimination for decades. The move to equalize benefits nudged them toward fairness. Since then, gays and lesbians have registered impressive progress in many domains. This progress is uneven, of course. Many gay, lesbian, and transgender Americans are still victims of prejudice, violence, and WMDs. This is especially true among poor and minority populations. Still, as I write this, a gay man, Tim Cook, is the chief executive of Apple, the most valuable company on earth. And if he so chooses, he has the constitutional right to marry a man.

Now that we've seen how corporations can move decisively to right a wrong in their hiring algorithms, why can't they make similar adjustments to the mathematical models wreaking havoc on our society, the WMDs?

Unfortunately, there's a glaring difference. Gay rights benefited in many ways from market forces. There was a highly educated and increasingly vocal gay and lesbian talent pool that companies were eager to engage. So they optimized their models to attract them. But they did this with the focus on the bottom line. Fairness, in most cases, was a by-product. At the same time, businesses across the country were starting to zero in on wealthy LGBT consumers, offering cruises, happy hours, and gay-themed TV shows. While inclusiveness no doubt caused grumbling in some pockets of intolerance, it also paid rich dividends.

Dismantling a WMD doesn't always offer such obvious payoff. While more fairness and justice would of course benefit society as a whole, individual companies are not positioned to reap the rewards. For most of them, in fact, WMDs appear to be highly effective. Entire business models, such as for-profit universities and payday loans, are built upon them. And when a software program successfully targets people desperate enough to pay 18 percent a month, those raking in the profits think it's working just fine.

The victims, of course, feel differently. But the greatest number of them—the hourly workers and unemployed, the people dragging low credit scores through life—are poor. Prisoners are powerless. And in our society, where money buys influence, these WMD victims are nearly voiceless. Most are disenfranchised politically. Indeed, all too often the poor are blamed for their poverty, their bad schools, and the crime that afflicts their neighborhoods. That's why few politicians even bother with antipoverty strategies. In the common view, the ills of poverty are more like a disease, and the effort—or at least the rhetoric—is to quarantine it

and keep it from spreading to the middle class. We need to think about how we assign blame in modern life and how models exacerbate this cycle.

But the poor are hardly the only victims of WMDs. Far from it. We've already seen how malevolent models can blacklist qualified job applicants and dock the pay of workers who don't fit a corporation's picture of ideal health. These WMDs hit the middle class as hard as anyone. Even the rich find themselves microtargeted by political models. And they scurry about as frantically as the rest of us to satisfy the remorseless WMD that rules college admissions and pollutes higher education.

It's also important to note that these are the early days. Naturally, payday lenders and their ilk start off by targeting the poor and the immigrants. Those are the easiest targets, the low-hanging fruit. They have less access to information, and more of them are desperate. But WMDs generating fabulous profit margins are not likely to remain cloistered for long in the lower ranks. That's not the way markets work. They'll evolve and spread, looking for new opportunities. We already see this happening as mainstream banks invest in peer-to-peer loan operations like Lending Club. In short, WMDs are targeting us all. And they'll continue to multiply, sowing injustice, until we take steps to stop them.

Injustice, whether based in greed or prejudice, has been with us forever. And you could argue that WMDs are no worse than the human nastiness of the recent past. In many cases, after all, a loan officer or hiring manager would routinely exclude entire races, not to mention an entire gender, from being considered for a mortgage or a job offer. Even the worst mathematical models, many would argue, aren't nearly that bad.

But human decision making, while often flawed, has one chief virtue. It can evolve. As human beings learn and adapt, we change, and so do our processes. Automated systems, by contrast,

stay stuck in time until engineers dive in to change them. If a Big Data college application model had established itself in the early 1960s, we still wouldn't have many women going to college, because it would have been trained largely on successful men. If museums at the same time had codified the prevalent ideas of great art, we would still be looking almost entirely at work by white men, the people paid by rich patrons to create art. The University of Alabama's football team, needless to say, would still be lily white.

Big Data processes codify the past. They do not invent the future. Doing that requires moral imagination, and that's something only humans can provide. We have to explicitly embed better values into our algorithms, creating Big Data models that follow our ethical lead. Sometimes that will mean putting fairness ahead of profit.

In a sense, our society is struggling with a new industrial revolution. And we can draw some lessons from the last one. The turn of the twentieth century was a time of great progress. People could light their houses with electricity and heat them with coal. Modern railroads brought in meat, vegetables, and canned goods from a continent away. For many, the good life was getting better.

Yet this progress had a gruesome underside. It was powered by horribly exploited workers, many of them children. In the absence of health or safety regulations, coal mines were death traps. In 1907 alone, 3,242 miners died. Meatpackers worked twelve to fifteen hours a day in filthy conditions and often shipped toxic products. Armour and Co. dispatched cans of rotten beef by the ton to US Army troops, using a layer of boric acid to mask the stench. Meanwhile, rapacious monopolists dominated the railroads, energy companies, and utilities and jacked up customers' rates, which amounted to a tax on the national economy.

Clearly, the free market could not control its excesses. So after journalists like Ida Tarbell and Upton Sinclair exposed these and other problems, the government stepped in. It established safety protocols and health inspections for food, and it outlawed child labor. With the rise of unions, and the passage of laws safeguarding them, our society moved toward eight-hour workdays and weekends off. These new standards protected companies that didn't want to exploit workers or sell tainted foods, because their competitors had to follow the same rules. And while they no doubt raised the costs of doing business, they also benefited society as a whole. Few of us would want to return to a time before they existed.

...

How do we start to regulate the mathematical models that run more and more of our lives? I would suggest that the process begin with the modelers themselves. Like doctors, data scientists should pledge a Hippocratic Oath, one that focuses on the possible misuses and misinterpretations of their models. Following the market crash of 2008, two financial engineers, Emanuel Derman and Paul Wilmott, drew up such an oath. It reads:

- ~ I will remember that I didn't make the world, and it doesn't satisfy my equations.
- ~ Though I will use models boldly to estimate value, I will not be overly impressed by mathematics.
- ~ I will never sacrifice reality for elegance without explaining why I have done so.
- ~ Nor will I give the people who use my model false comfort about its accuracy. Instead, I will make explicit its assumptions and oversights.

~ I understand that my work may have enormous effects on society and the economy, many of them beyond my comprehension.

That's a good philosophical grounding. But solid values and self-regulation rein in only the scrupulous. What's more, the Hippocratic Oath ignores the on-the-ground pressure that data scientists often confront when bosses push for specific answers. To eliminate WMDs, we must advance beyond establishing best practices in our data guild. Our laws need to change, too. And to make that happen we must reevaluate our metric of success.

Today, the success of a model is often measured in terms of profit, efficiency, or default rates. It's almost always something that can be counted. What should we be counting, though? Consider this example. When people look for information about food stamps on a search engine, they are often confronted with ads for go-betweens, like FindFamilyResources, of Tempe, Arizona. Such sites look official and provide links to real government forms. But they also gather names and e-mail addresses for predatory advertisers, including for-profit colleges. They rake in lead generation fees by providing a superfluous service to people, many of whom are soon targeted for services they can ill afford.

Is the transaction successful? It depends on what you count. For Google, the click on the ad brings in a quarter, fifty cents, or even a dollar or two. That's a success. Naturally, the lead generator also makes money. And so it looks as though the system is functioning efficiently. The wheels of commerce are turning.

Yet from society's perspective, a simple hunt for government services puts a big target on the back of poor people, leading a certain number of them toward false promises and high-interest loans. Even considered strictly from an economic point of view,

it's a drain on the system. The fact that people need food stamps in the first place represents a failing of the market economy. The government, using tax dollars, attempts to compensate for it, with the hope that food stamp recipients will eventually be able to fully support themselves. But the lead aggregators push them toward needless transactions, leaving a good number of them with larger deficits, and even more dependent on public assistance. The WMD, while producing revenue for search engines, lead aggregators, and marketers, is a leech on the economy as a whole.

A regulatory system for WMDs would have to measure such hidden costs, while also incorporating a host of non-numerical values. This is already the case for other types of regulation. Though economists may attempt to calculate costs for smog or agricultural runoff, or the extinction of the spotted owl, numbers can never express their value. And the same is often true of fairness and the common good in mathematical models. They're concepts that reside only in the human mind, and they resist quantification. And since humans are in charge of making the models, they rarely go the extra mile or two to even try. It's just considered too difficult. But we need to impose human values on these systems, even at the cost of efficiency. For example, a model might be programmed to make sure that various ethnicities or income levels are represented within groups of voters or consumers. Or it could highlight cases in which people in certain zip codes pay twice the average for certain services. These approximations may be crude, especially at first, but they're essential. Mathematical models should be our tools, not our masters.

The achievement gap, mass incarceration, and voter apathy are big, nationwide problems that no free market nor mathematical algorithm will fix. So the first step is to get a grip on our techno-utopia, that unbounded and unwarranted hope in what

algorithms and technology can accomplish. Before asking them to do better, we have to admit they can't do everything.

To disarm WMDs, we also need to measure their impact and conduct algorithmic audits. The first step, before digging into the software code, is to carry out research. We'd begin by treating the WMD as a black box that takes in data and spits out conclusions. This person has a medium risk of committing another crime, this one has a 73 percent chance of voting Republican, this teacher ranks in the lowest decile. By studying these outputs, we could piece together the assumptions behind the model and score them for fairness.

Sometimes, it is all too clear from the get-go that certain WMDs are only primitive tools, which hammer complexity into simplicity, making it easier for managers to fire groups of people or to offer discounts to others. The value-added model used in New York public schools, for example, the one that rated Tim Clifford a disastrous 6 one year and then a high-flying 96 a year later, is a statistical farce. If you plot year-to-year scores on a chart, the dots are nearly as randomly placed as hydrogen atoms in a room. Many of the math students in those very schools could study those statistics for fifteen minutes and conclude, with confidence, that the scores measure nothing. Good teachers, after all, tend to be good one year after the next. Unlike, say, relief pitchers in baseball, they rarely have great seasons followed by disasters. (And also unlike relief pitchers, their performance resists quantitative analysis.)

There's no fixing a backward model like the value-added model. The only solution in such a case is to ditch the unfair system. Forget, at least for the next decade or two, about building tools to measure the effectiveness of a teacher. It's too complex to model, and the only available data are crude proxies. The model is simply not good enough yet to inform important decisions about the people we trust to teach our children. That's a job that requires

subtlety and context. Even in the age of Big Data, it remains a problem for humans to solve.

Of course, the human analysts, whether the principal or administrators, should consider lots of data, including the students' test scores. They should incorporate positive feedback loops. These are the angelic cousins of the pernicious feedback loops we've come to know so well. A positive loop simply provides information to the data scientist (or to the automatic system) so that the model can be improved. In this case, it's simply a matter of asking teachers and students alike if the evaluations make sense for them, if they understand and accept the premises behind them. If not, how could they be enhanced? Only when we have an ecosystem with positive feedback loops can we expect to improve teaching using data. Until then it's just punitive.

It is true, as data boosters are quick to point out, that the human brain runs internal models of its own, and they're often tinged with prejudice or self-interest. So its outputs—in this case, teacher evaluations—must also be audited for fairness. And these audits have to be carefully designed and tested by human beings, and afterward automated. In the meantime, mathematicians can get to work on devising models to help teachers measure their own effectiveness and improve.

Other audits are far more complicated. Take the criminal recidivism models that judges in many states consult before sentencing prisoners. In these cases, since the technology is fairly new, we have a before and an after. Have judges' sentencing patterns changed since they started receiving risk analysis from the WMD? We'll see, no doubt, that a number of the judges ran similarly troubling models in their heads long before the software arrived, punishing poor prisoners and minorities more severely than others. In some of those cases, conceivably, the software might temper their judgments. In others, not. But with enough data,

patterns will become clear, allowing us to evaluate the strength and the tilt of the WMD.

If we find (as studies have already shown) that the recidivism models codify prejudice and penalize the poor, then it's time to take a look at the inputs. In this case, they include loads of birds-of-a-feather connections. They predict an individual's behavior on the basis of the people he knows, his job, and his credit rating—details that would be inadmissible in court. The fairness fix is to throw out that data.

But wait, many would say. Are we going to sacrifice the accuracy of the model for fairness? Do we have to dumb down our algorithms?

In some cases, yes. If we're going to be equal before the law, or be treated equally as voters, we cannot stand for systems that drop us into different castes and treat us differently.\* Companies like Amazon and Netflix can plunk their paying customers into little buckets and optimize them all they want. But the same algorithm cannot deliver justice or democracy.

Movements toward auditing algorithms are already afoot. At Princeton, for example, researchers have launched the Web Transparency and Accountability Project. They create software robots that masquerade online as people of all stripes—rich, poor, male, female, or suffering from mental health issues. By study-

\* You might think that an evenhanded audit would push to eliminate variables such as race from the analysis. But if we're going to measure the impact of a WMD, we need that data. Currently, most of the WMDs avoid directly tracking race. In many cases, it's against the law. It is easier, however, to expose racial discrimination in mortgage lending than in auto loans, because mortgage lenders are required to ask for the race of the applicant, while auto lenders are not. If we include race in the analysis, as the computer scientist Cynthia Dwork has noted, we can quantify racial injustice where we find it. Then we can publicize it, debate the ethics, and propose remedies. Having said that, race is a social construct and as such is difficult to pin down even when you intend to, as any person of mixed race can tell you.

ing the treatment these robots receive, the academics can detect biases in automated systems from search engines to job placement sites. Similar initiatives are taking root at universities like Carnegie Mellon and MIT.

Academic support for these initiatives is crucial. After all, to police the WMDs we need people with the skills to build them. Their research tools can replicate the immense scale of the WMDs and retrieve data sets large enough to reveal the imbalances and injustice embedded in the models. They can also build crowdsourcing campaigns, so that people across society can provide details on the messaging they're receiving from advertisers or politicians. This could illuminate the practices and strategies of microtargeting campaigns.

Not all of them would turn out to be nefarious. Following the 2012 presidential election, for example, ProPublica built what it called a Message Machine, which used crowdsourcing to reverse-engineer the model for the Obama campaign's targeted political ads. Different groups, as it turned out, heard glowing remarks about the president from different celebrities, each one presumably targeted for a specific audience. This was no smoking gun. But by providing information and eliminating the mystery behind the model, the Message Machine reduced (if only by a tad) grounds for dark rumors and suspicion. That's a good thing.

If you consider mathematical models as the engines of the digital economy—and in many ways they are—these auditors are opening the hoods, showing us how they work. This is a vital step, so that we can equip these powerful engines with steering wheels—and brakes.

Auditors face resistance, however, often from the web giants, which are the closest thing we have to information utilities. Google, for example, has prohibited researchers from creating scores of

fake profiles in order to map the biases of the search engine.\* If the company does in fact carry out bias audits, its preference is to keep them internal. That way they shield the algorithm's inner workings, and its prejudices, from outsiders. But insiders, suffering as we all do from confirmation bias, are more likely to see what they expect to find. They might not ask the most probing questions. And if they find injustices that appear to boost Google's bottom line . . . well, that could lead to uncomfortable discussions, ones they'd certainly want to keep out of the public light. So there are powerful business arguments for secrecy. But as the public learns more about WMDs, and demands more accountability from these utilities, Google, I'm hoping, will have little choice but to let outsiders in.

Facebook, too. The social network's rigorous policy to tie users to their real names severely limits the research outsiders can carry out there. The real-name policy is admirable in many ways, not least because it pushes users to be accountable for the messages they post. But Facebook also must be accountable to all of us—which means opening its platform to more data auditors.

The government, of course, has a powerful regulatory role to play, just as it did when confronted with the excesses and tragedies of the first industrial revolution. It can start by adapting and then enforcing the laws that are already on the books.

As we discussed in the chapter on credit scores, the civil rights laws referred to as the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA) were meant to ensure fairness in credit scoring. The FCRA guarantees that a consumer can see the data going into their score and correct any errors, and the ECOA prohibits linking race or gender to a person's score.

\* Google has expressed interest in working to eliminate bias from its algorithm, and some Google employees briefly talked to me about this. One of the first things I tell them is to open the platform to more outside researchers.

These regulations are not perfect, and they desperately need updating. Consumer complaints are often ignored, and there's nothing explicitly keeping credit-scoring companies from using zip codes as proxies for race. Still, they offer a good starting point. First, we need to demand transparency. Each of us should have the right to receive an alert when a credit score is being used to judge or vet us. And each of us should have access to the information being used to compute that score. If it is incorrect, we should have the right to challenge and correct it.

Next, the regulations should expand to cover new types of credit companies, like Lending Club, which use newfangled e-scores to predict the risk that we'll default on loans. They should not be allowed to operate in the shadows.

The Americans with Disabilities Act (ADA), which protects people with medical issues from being discriminated against at work, also needs an update. The bill currently prohibits medical exams as part of an employment screening. But we need to update it to take into account Big Data personality tests, health scores, and reputation scores. They all sneak around the law, and they shouldn't be able to. One possibility already under discussion would extend protection of the ADA to include "predicted" health outcomes down the road. In other words, if a genome analysis shows that a person has a high risk for breast cancer, or for Alzheimer's, that person should not be denied job opportunities.

We must also expand the Health Insurance Portability and Accountability Act (HIPAA), which protects our medical information, in order to cover the medical data currently being collected by employers, health apps, and other Big Data companies. Any health-related data collected by brokers, such as Google searches for medical treatments, must also be protected.

If we want to bring out the big guns, we might consider moving toward the European model, which stipulates that any data

collected must be approved by the user, as an opt-in. It also prohibits the reuse of data for other purposes. The opt-in condition is all too often bypassed by having a user click on an inscrutable legal box. But the “not reusable” clause is very strong: it makes it illegal to sell user data. This keeps it from the data brokers whose dossiers feed toxic e-scores and microtargeting campaigns. Thanks to this “not reusable” clause, the data brokers in Europe are much more restricted, assuming they follow the law.

Finally, models that have a significant impact on our lives, including credit scores and e-scores, should be open and available to the public. Ideally, we could navigate them at the level of an app on our phones. In a tight month, for example, a consumer could use such an app to compare the impact of unpaid phone and electricity bills on her credit score and see how much a lower score would affect her plans to buy a car. The technology already exists. It’s only the will we’re lacking.

...

On a summer day in 2013, I took the subway to the southern tip of Manhattan and walked to a large administrative building across from New York’s City Hall. I was interested in building mathematical models to help society—the opposite of WMDs. So I’d signed on as an unpaid intern in a data analysis group within the city’s Housing and Human Services Departments. The number of homeless people in the city had grown to sixty-four thousand, including twenty-two thousand children. My job was to help create a model that would predict how long a homeless family would stay in the shelter system and to pair each family with the appropriate services. The idea was to give people what they needed to take care of themselves and their families and to find a permanent home.

My job, in many ways, was to help come up with a recidivism

model. Much like the analysts building the LSI-R model, I was interested in the forces that pushed people back to shelters and also those that led them to stable housing. Unlike the sentencing WMD, though, our small group was concentrating on using these findings to help the victims and to reduce homelessness and despair. The goal was to create a model for the common good.

On a separate but related project, one of the other researchers had found an extremely strong correlation, one that pointed to a solution. A certain group of homeless families tended to disappear from shelters and never return. These were the ones who had been granted vouchers under a federal affordable housing program called Section 8. This shouldn’t have been too surprising. If you provide homeless families with affordable housing, not too many of them will opt for the streets or squalid shelters.

Yet that conclusion might have been embarrassing to then-mayor Michael Bloomberg and his administration. With much fanfare, the city government had moved to wean families from Section 8. It instituted a new system called Advantage, which limited subsidies to three years. The idea was that the looming expiration of their benefits would push poor people to make more money and pay their own way. This proved optimistic, as the data made clear. Meanwhile, New York’s booming real estate market was driving up rents, making the transition even more daunting. Families without Section 8 vouchers streamed back into the shelters.

The researcher’s finding was not welcome. For a meeting with important public officials, our group prepared a PowerPoint presentation about homelessness in New York. After the slide with statistics about recidivism and the effectiveness of Section 8 was put up, an extremely awkward and brief conversation took place. Someone demanded the slide be taken down. The party line prevailed.

While Big Data, when managed wisely, can provide important insights, many of them will be disruptive. After all, it aims to find patterns that are invisible to human eyes. The challenge for data scientists is to understand the ecosystems they are wading into and to present not just the problems but also their possible solutions. A simple workflow data analysis might highlight five workers who appear to be superfluous. But if the data team brings in an expert, they might help discover a more constructive version of the model. It might suggest jobs those people could fill in an optimized system and might identify the training they'd need to fill those positions. Sometimes the job of a data scientist is to know when you don't know enough.

As I survey the data economy, I see loads of emerging mathematical models that might be used for good and an equal number that have the potential to be great—if they're not abused. Consider the work of Mira Bernstein, a slavery sleuth. A Harvard PhD in math, she created a model to scan vast industrial supply chains, like the ones that put together cell phones, sneakers, or SUVs, to find signs of forced labor. She built her slavery model for a nonprofit company called Made in a Free World. Its goal is to use the model to help companies root out the slave-built components in their products. The idea is that companies will be eager to free themselves from this scourge, presumably because they oppose slavery, but also because association with it could devastate their brand.

Bernstein collected data from a number of sources, including trade data from the United Nations, statistics about the regions where slavery was most prevalent, and detailed information about the components going into thousands of industrial products, and incorporated it all into a model that could score a given product from a certain region for the likelihood that it was made using slave labor. “The idea is that the user would contact his supplier

and say, ‘Tell me more about where you’re getting the following parts of your computers,’” Bernstein told *Wired* magazine. Like many responsible models, the slavery detector does not overreach. It merely points to suspicious places and leaves the last part of the hunt to human beings. Some of the companies find, no doubt, that the suspected supplier is legit. (Every model produces false positives.) That information comes back to Made in a Free World, where Bernstein can study the feedback.

Another model for the common good has emerged in the field of social work. It’s a predictive model that pinpoints households where children are most likely to suffer abuse. The model, developed by Eckerd, a child and family services nonprofit in the southeastern United States, launched in 2013 in Florida’s Hillsborough County, an area encompassing Tampa. In the previous two years, nine children in the area had died from abuse, including a baby who was thrown out a car window. The modelers included 1,500 child abuse cases in their database, including the fatalities. They found a number of markers for abuse, including a boyfriend in the home, a record of drug use or domestic violence, and a parent who had been in foster care as a child.

If this were a program to target potential criminals, you can see right away how unfair it could be. Having lived in a foster home or having an unmarried partner in the house should not be grounds for suspicion. What’s more, the model is much more likely to target the poor—and to give a pass to potential abuse in wealthy neighborhoods.

Yet if the goal is not to punish the parents, but instead to provide help to children who might need it, a potential WMD turns benign. It funnels resources to families at risk. And in the two years following implementation of the model, according to the *Boston Globe*, Hillsborough County suffered no fatalities from child abuse.

Models like this will abound in coming years, assessing our risk of osteoporosis or strokes, swooping in to help struggling students with calculus II, even predicting the people most likely to suffer life-altering falls. Many of these models, like some of the WMDs we've discussed, will arrive with the best intentions. But they must also deliver transparency, disclosing the input data they're using as well as the results of their targeting. And they must be open to audits. These are powerful engines, after all. We must keep our eyes on them.

Data is not going away. Nor are computers—much less mathematics. Predictive models are, increasingly, the tools we will be relying on to run our institutions, deploy our resources, and manage our lives. But as I've tried to show throughout this book, these models are constructed not just from data but from the choices we make about which data to pay attention to—and which to leave out. Those choices are not just about logistics, profits, and efficiency. They are fundamentally moral.

If we back away from them and treat mathematical models as a neutral and inevitable force, like the weather or the tides, we abdicate our responsibility. And the result, as we've seen, is WMDs that treat us like machine parts in the workplace, that blackball employees and feast on inequities. We must come together to police these WMDs, to tame and disarm them. My hope is that they'll be remembered, like the deadly coal mines of a century ago, as relics of the early days of this new revolution, before we learned how to bring fairness and accountability to the age of data. Math deserves much better than WMDs, and democracy does too.